

IN THE CIRCUIT COURT FOR GARRETT COUNTY, MARYLAND

BRANDON LEE ROANE, an individual,
on behalf of himself all others similarly situated,)
c/o Arnold Abraham, Esq.)
The CyberLaw Group)
220 N. Liberty Street)
Baltimore MD 21201)
Plaintiff,)
v.)
GRMC, INC., doing business as)
“Garrett Regional Medical Center”)
251 N. 4th Street)
Oakland, Maryland 21550-1375)
Serve on Registered Agent:) JURY TRIAL DEMANDED
Mark Boucot)
251 N. 4th Street)
Oakland, Maryland 21550-1375)
Defendant.)
Case No.: C-11-CV-23-000177

CLASS ACTION COMPLAINT

Plaintiff Brandon Lee Roane, an individual (“Mr. Roane” or “Named Plaintiff”), on behalf of himself and others similarly situated, by and through his undersigned attorneys, sues Defendant, GRMC, Inc., doing business as “Garrett Regional Medical Center” (“GRMC”), and states as follows:

I. INTRODUCTION

1. This class action seeks monetary and injunctive relief to redress injuries resulting from Defendant's negligence and wrongful acts related to a computer data breach that exposed the personal data of individuals who were patients of GRMC.

II. VENUE AND JURISDICTION

2. This Court has subject matter jurisdiction over this action as the amount in controversy exceeds \$25,000, exclusive of interest and costs, and the relief sought includes equitable, declaratory, and injunctive relief for which the Circuit Court has exclusive jurisdiction.

3. This Court has personal jurisdiction over the present matter because Defendant contracted to provide services in Maryland, or regularly conduct business in Maryland.

4. Maryland is also where a substantial portion of the events or omissions giving rise to this claim occurred and a substantial portion of the property that is the subject of this action is situated.

5. Venue is also proper in this Court because the named Defendant is located in Garrett County, Maryland and/or carries-on business activities in Maryland. The cause of action arose in this venue.

III. ALLEGATIONS AS TO PARTIES

6. At all times material hereto, Mr. Roane was *sui juris* and a resident of Garrett County, Maryland.

7. GRMC is a corporation doing business in Garrett County, Maryland.

8. GRMC is a nonprofit health enterprise which provides services throughout West Virginia and portions of the surrounding states of Maryland, Ohio, and Pennsylvania, including Garrett Regional Medical Center (“Garrett Regional”) in Oakland, Maryland.

9. Garrett Regional has 55 inpatient beds; a four-bed intensive care unit; a 10-bed subacute rehabilitation unit; a family-centered maternity suite; a 13-bed outpatient surgical unit with a four-bed surgical suite.

10. Garrett Regional has a professional staff of 500 physicians and allied health

professionals.

11. GRMC has been recognized as one of the top 20 rural and community hospitals in the United States. *See,* [*https://www.forevercumberland.com/2021/04/04/grmc-in-top-20-rural-community-hospitals/*](https://www.forevercumberland.com/2021/04/04/grmc-in-top-20-rural-community-hospitals/).

12. One of the factors that contribute to GRMC's high ratings is their use of automatic computer systems. GRMC earned the highest possible rating in one category for having a well-functioning Computer Physician Order Entry Systems.

See, [*https://www.hospitalssafetygrade.org/table-details/garrett-regional-medical-center*](https://www.hospitalssafetygrade.org/table-details/garrett-regional-medical-center).

13. At all times material hereto, Mr. Garrett was a patient of Garrett Regional and entrusted his personal information and medical records to Garrett Regional.

IV. FACTUAL ALLEGATIONS

A. DETAILS OF DATA AND PRIVACY BREACH

14. In May 2023, Defendant had a breach in their computer network security that affected the private information of Mr. Roane and hundreds of other patients.

15. As a result of the breach, the Protected Health Information (“PHI”) of Mr. Roane and hundreds of other patients was accessed and disclosed in an unauthorized manner.

16. As a result of the breach, the Personal Information (“PI”) of Mr. Roane and hundreds of other patients was accessed and disclosed in an unauthorized manner.

17. On information and belief, healthcare organizations, including Defendant, use MOVEit products to deliver scalable, secure, and compliant patient care and business services, including healthcare billing, insurance-eligibility inquiries, healthcare claims, detailed audit logs, appointment reminders, patient surveys, and patient retrieval of medical records.

18. It is unknown whether GRMC took action in response, including disconnecting the

server that utilized the MOVEit software.

19. Based on the best information available to Plaintiff, more than one thousand (1000) patients had their information accessed in the data breach.

20. Section 13402(e)(4) of the HITECH Act requires Health and Human Services (HHS) to post a list of breaches of unsecured protected health information affecting 500 or more individuals.

21. As of the date hereof, the HHS website does not indicate that GRMC submitted a notice of a breach.

22. According to GRMC, the personal information downloaded included the name and date of birth of the patient, description of medical services, and other medical information.

23. The information listed in the above paragraph fits within the category of medical health records information and protected health information (“PHI”).

24. Breaches of PHI are subject to the HIPAA.

25. The information listed in the above paragraph fits in the category of financial information and Personal Information (“PI”).

26. Breaches of PI are subject to the provisions of the Maryland Personal Information Privacy Act (“MD PIPA”).

27. Defendant did not comply with breach notification requirements of MD PIPA or HIPAA requirements.

28. GRMC was previously warned about the threat they faced that led to this breach and failed to take reasonable measures to Plaintiff information.

29. The latest vulnerability that GRMC was warned of in MOVEit, follows previous MOVEit vulnerabilities as reported in the National Vulnerability Database, including CVE-2023-

30394 (May 19, 2023), CVE-2021-37614 (August 17, 2021), CVE-2021-33894 (June 22, 2021), CVE-2021-31827 (May 25, 2021), and CVE-2020-12677 (May 19, 2020).

30. On information and belief, the Cl0p ransomware gang was the source of the breach.

31. On February 22, 2023, the Health Sector Cybersecurity Coordination Center (“HC3”) published a sector alert titled “Cl0p Allegedly Targets Healthcare Industry in Data Breach.”

32. HC3 published an additional alert on April 28, 2023, regarding the threat from Cl0p.

33. HC3 was created by the Department of Health and Human Services to aid in the protection of vital, controlled, healthcare-related information, and to ensure that cybersecurity information sharing is coordinated across the health and public health sectors.

34. In October 2022, the Maryland Health Care Commission published a report titled “Health Care Data Breach Trends 2018-2021” which provided warning of this type of threat.

35. According to the Maryland Health Care Commission, the proliferation of health information technology presents new vulnerabilities and increases the risk of a breach for health care organizations.

36. On information and belief, GRMC did not adequately implement the 10 Mitigating Practices identified by the 405(d) Task Group and published in the “Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients.”

37. The 405(d) Program was established under the Cybersecurity Act of 2015 to strengthen the cybersecurity posture of the healthcare and public health sector. It is a collaborative effort between industry and the federal government to align healthcare industry security practices to develop consensus-based guidelines, practices, and methodologies to strengthen the healthcare

and public health sector's cybersecurity posture against cyber threats. <https://405d.hhs.gov>.

38. The necessary actions to mitigate the risk of the type of incident that occurred were known to GRMC and within their capacity to reasonably implement.

39. On information and belief, GRMC has been well aware of the risk posed to patient records and health information such as what was exposed in this case.

40. For many years, cybersecurity risk in the healthcare industry has been widely recognized as significant and more than 110 million records were compromised in 2015 alone according to the Office of Civil Rights (OCR) under Health and Human Services. *See*, “Has health care hacking become an epidemic?” <https://www.pbs.org/newshour/science/has-health-care-hacking-become-an-epidemic>

41. According to Dr. Avi Rubin, a former senior cybersecurity employee of Johns Hopkins University, the health care sector was the “absolute worst” in terms of cybersecurity problems and “[t]heir data security practices were so far below every other industry.” *Id.*

42. “Electronic health records are 100 times more valuable than stolen credit cards,” according to James Scott, co-founder, and senior fellow at the Institute for Critical Infrastructure Technology (ICIT) in Washington D.C. *Id.*

43. A single Medicare or Medicaid electronic health record can fetch a \$500 price tag on dark web forums. *Id.*

44. Experian, the global information service, estimates that health records are worth up to 10 times more than credit card numbers on the black market. *Id.*

45. For at least seven years, cybersecurity experts have recommended policies like encrypting all patient data and limiting who has permission to view medical charts as reasonable defense measures. *Id.*

46. On information and belief, the patient data accessed in this breach was not encrypted.

V. INJURY AND HARM TO CLASS

A. GENERAL HARM

47. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have sustained and will continue to sustain economic loss and other harms. They have experienced and/or face an increased risk of experiencing the following forms of injuries:

- a. Direct and indirect negative impacts on health and welfare, leading to permanent and irreversible consequences in their personal and professional lives:
 - i. theft of their Personal Information;
 - ii. publication of their Personal Information to the Dark Web;
 - iii. damages to and diminution in value of their Personal Information;
 - iv. loss of the opportunity to control how their Personal Information is used;
 - v. time spent on efforts to research how to prevent, detect, contest, and recover from misuse of Personal Information;
 - vi. Emotional distress from the unauthorized disclosure of information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff.
 - vii. Continued risk of exposure to hackers and thieves of their information, which remains in Defendant's possession and is subject to further breaches so long as GRMC fails to undertake appropriate and adequate measures to protect Class members' data.

- b. Costs associated and time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the breach, including:
- i. money and time expended to prevent, detect, contest, and repair identity theft, fraud, and other unauthorized uses of Personal Information, including by identifying, disputing, and seeking reimbursement for fraudulent activity and canceling compromised financial accounts and associated payment cards; imposing withdrawal and purchase limits on compromised accounts and other accounts subject to potential compromise; enrolling in credit monitoring and identity theft protection services;
 - ii. money and time lost as a result of fraudulent access to and use of their financial accounts, and fraudulent charges, loss of use of and access to their financial accounts and/or credit, including loss of use and access to their financial account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;
 - iii. money and time expended to periodically order credit reports and place temporary freezes on credit, and to
 - iv. money and time expended to avail themselves of assets and/or credit frozen or flagged due to misuse;
 - v. impairment of their credit scores, ability to borrow, and/or ability to obtain credit;

- vi. anticipated future costs from the purchase of credit monitoring and identity theft protection services once the temporary services being offered by Defendant expire;
- c. Costs associated with additional computer security needed due to increased personal vulnerability to cyber threats, including the enhanced risk of potential phishing attacks specifically crafted based on the extensive Personal Information revealed, such as increased costs for anti-malware software and network security software and monitoring services on all of Plaintiff's electronic devices, as well as increased time and effort to monitor for potential intrusions and respond to cyber security incidents on their personal devices and networks.

48. Plaintiff was/will be required to spend a substantial amount of time responding to and rectifying the losses incurred.

49. Plaintiff alleges that any and all time spent responding to and rectifying the breaches and losses described herein is properly valued at a fair hourly rate, multiplied by the time expended.

50. The full impact of the violation of privacy through this breach can only be measured over the course of the lifetime of those affected.

51. At least one study has shown the average cost incurred in trying to resolve a medical identity theft incident is more than \$18,660. See, *National Study on Medical Identity Theft*, Ponemon Institute.¹

¹

<https://www.ponemon.org/local/upload/file/2013%20Medical%20Identity%20Theft%20Report%20FINAL%2011.pdf> (last visited on November 14, 2023)

52. As a direct and proximate result of the unauthorized access and disclosure of his private information, Plaintiff became severely stressed and suffered anxiety, including physical manifestations.

53. According to the Maryland Health Care Commission, health care is among the sectors most targeted by cyber-attacks due to the value of medical information as compared to financial or other information.

VI. CLASS REPRESENTATION ALLEGATIONS

A. STATEMENT OF MAINTAINABLE CLASS CLAIMS

54. Pursuant to Md. Rule 2-231, Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Md. Rule 2-231(b)(2) and (3),

B. DEFINITION OF CLASS

55. The “Class” that Plaintiff seeks to represent is defined as follows:

All persons whose Private Information was maintained by GRMC and accessed or acquired during the Data Breach as a result of the exploitation of the MOVEit Application vulnerability.

56. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant’s parent entities, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

57. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

C. ALLEGATIONS OF NUMEROSITY

58. Pursuant to Md. Rule 2-231(a)(1), the Class Members are so numerous that the joinder of all members is impracticable. Upon information and belief, there are thousands of individuals whose Private Information may have been improperly accessed in the Data Breach, and the Class is readily identifiable within Defendant's records.

D. IDENTIFICATION OF COMMON QUESTIONS OF LAW OR FACT

59. Pursuant to Md. Rule 2-231(a)(2), the questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

- a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;
- b. Whether Defendant had a duty not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant had duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;
- e. Whether and when Defendant actually learned of the Data Breach;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII and PHI had been compromised;
- h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;
- k. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant' wrongful conduct;
- l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant' wrongful conduct; and
- m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

E. ALLEGATIONS OF TYPICALITY

60. Pursuant to Md. Rule 2-231(a)(3), Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach due to Defendant's misfeasance.

F. ADEQUACY OF REPRESENTATION

61. Pursuant to Md. Rule 2-231(a)(4), Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights Plaintiff has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation. *See, Whitaker v. Navy Federal Credit Union*, 2010 WL 3928616, at *6 (D. Md. Oct. 4, 2010) [in setting hourly rate at \$450 in 2010, Judge Bennett of this Court stated: “[t]hough Murphy's hourly rate is above the applicable range, his wealth of experience in litigating class actions justifies his high rate”]. Moreover, Plaintiff has retained

counsel with extensive cyber-security expertise, including the past senior executive at the Department of Defense, U.S. Cyber Command. *See, https://www.thecyberlawteam.com/about.*

G. PREDOMINANCE

62. Pursuant to Md. Rule 2-231(b)(2), Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that the Plaintiff's and Class Members' data was maintained and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

H. SUPERIORITY

63. Pursuant to Md. Rule 2-231 (b)(3), Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

64. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

65. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, including its privacy policy, uniform methods of data collection, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

66. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

67. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Petition.

68. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

69. Likewise, under Md. Rule 2-231(c)(4), the following issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in obtaining, storing, collecting, maintaining, using, and/or safeguarding their Private Information;
- b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in obtaining, storing, collecting, maintaining, using, and/or safeguarding their Private Information;
- c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;
- e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- f. Whether Defendant's data security practices related to its MOVEit Application prior to and during the Data Breach complied with applicable data security laws and regulations;
- g. Whether Defendant's data security practices related to its MOVEit Application prior to and during the Data Breach were consistent with industry standards;
- h. Whether hackers obtained Class Members' Private Information via the Data Breach;

- i. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members; and
- j. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I – ACTION FOR NEGLIGENCE

70. Plaintiff realleges and incorporates by reference each and every allegation set forth above.

71. GRMC had a duty to the Plaintiff to maintain data security measures consistent with statutory and industry standards.

72. GRMC had a duty to the Plaintiff to design, maintain, or test security systems to ensure that Plaintiff's Personal Information (PI), Personally Identifiable Information (PII), and Protected Health Information (PHI) in their possession was adequately secured and protected.

73. GRMC had a duty to the Plaintiff to implement processes that would detect a breach of its security system in a timely manner.

74. On information and belief, GRMC breached each of these duties, as evidenced by the events described in this complaint.

75. GRMC knew or should have known of the risks inherent in collecting, maintaining, and storing PI, PII, PHI and Medical Records of Plaintiff and the heightened risk of doing so without adequate security systems and protocols.

76. GRMC owed a duty to Plaintiff to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PI, PII, PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

77. On information and belief, GRMC breached that duty, as evidenced by the events described in this complaint.

78. GRMC had a duty to prevent foreseeable harm to Plaintiff. This duty existed because Plaintiff were foreseeable and probable victims of inadequate security practices.

79. It was foreseeable that Plaintiff would be harmed by the failure to protect his PI, PII, and PHI because hackers routinely attempt to steal such information and use it for nefarious purposes.

80. GRMC breached the duties it owed to Plaintiff to keep his information secure. But for GRMC's wrongful and negligent breach of its duties owed to Plaintiff, PI, PII, and PHI would not have been compromised.

81. On information and belief, GRMC had numerous opportunities in advance of the breach to reasonably implement adequate cyber security measures as part of their duties to the Plaintiff but failed to do so.

82. Because GRMC is covered by HIPAA (45 C.F.R. § 160.102), it is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

83. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

84. HIPAA requires GRMC to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronically protected health information." 45 C.F.R. § 164.302.

85. HIPAA's Security Rule requires GRMC to ensure the confidentiality of

electronically protected health information it maintains.

86. HIPAA Security Rule requires GRMC to protect against any reasonably anticipated threats or hazards to the security protected health information it maintains.

87. HIPAA also requires GRMC to “review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronically protected health information” under 45 C.F.R. § 164.306(e), and to “[i]mplement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights.” 45 C.F.R. § 164.312(a)(1).

88. On information and belief, GRMC failed to comply with requirements of HIPAA’s security rule described above and breached its duties to Plaintiff as described under its HIPAA obligations.

89. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires GRMC to provide notice of the breach to each affected individual without unreasonable delay.

90. On information and belief, Defendant failed to maintain data security measures consistent with statutory and industry standards.

91. On information and belief, Defendant failed to implement the following measures recommended by the FBI to prevent and detect ransomware attacks, including the attack that resulted in the breach:²

² See “How to Protect Your Networks from RANSOMWARE,” at 3, *available at* <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited on August 23, 2023)

- a. Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered;
- b. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing;
- c. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users;
- d. Configure firewalls to block access to known malicious IP addresses;
- e. Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system;
- f. Set anti-virus and anti-malware programs to conduct regular scans automatically;
- g. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary;
- h. Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have written access to those files, directories, or shares;
- i. Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications;

- j. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder;
- k. Consider disabling Remote Desktop protocol (RDP) if it is not being used;
- l. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy;
- m. Execute operating system environments or specific programs in a virtualized environment; and
- n. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

92. On information and belief, Defendant failed to implement the measures recommended by the United States Cybersecurity & Infrastructure Security Agency to prevent and detect ransomware attacks, including the attack that resulted in the breach.³

93. On information and belief, Defendant failed to implement the measures recommended by the Microsoft Threat Protection Intelligence Team to prevent and detect ransomware attacks, including the attack that resulted in the breach.⁴

94. As a direct and proximate result of GRMC' negligence and breach of duties, Plaintiff sustained and will continue to sustain economic loss and other harms.

³ See Protecting Your Networks from Ransomware publication <https://www.cisa.gov/resources-tools/resources/protecting-your-networks-ransomware> (last visited August 13, 2023).

⁴ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited August 13, 2023).

95. Plaintiff experienced and/or face an increased risk of experiencing the following forms of injuries:

- a. direct and indirect negative impacts on health and welfare, leading to permanent and irreversible consequences in his personal and professional life; and
- b. emotional distress, mental pain and suffering due to exposure of highly sensitive private information.

96. Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Personal Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant had a duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were foreseeable and probable victims of inadequate security practices.

97. In fact, not only was it foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their Personal Information, because hackers routinely attempt to steal such information and use it for nefarious purposes, but Defendant also knew that it was more likely than not Plaintiff and other Class Members would be harmed, and in fact, suffered harm as identified above.

98. Defendant breached the duties they owed to Plaintiff and Class Members to keep their information secure. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, and without any wrongdoing on the part of Plaintiff or Class Members, Plaintiff's and Class Members' Personal Information would not have been compromised.

99. Plaintiff relies on the doctrines of actual and apparent agency, res ipsa loquitur, and respondeat superior where applicable.

100. GRMC's negligence caused Plaintiff to suffer harm as described above and actual damages in an amount to be determined at trial.

**COUNT II – ACTION FOR VIOLATION OF MARYLAND MEDICAL RECORDS ACT
(DUTY TO HOLD CONFIDENTIAL AND DUTY TO DISCLOSE
A MEDICAL RECORD) MD. CODE §§ 4-301– 4-309.**

101. Plaintiff realleges and incorporates by reference each and every allegation set forth above.

102. GRMC is subject to the requirements of this act, including the duty to keep the medical record of a patient confidential under § 4-302 (a).

103. A health care provider or any other person is in violation of this act if they disclose a medical record in violation of this subtitle under § 4-309 (c) (2).

104. The act provides for additional specified civil penalties and fines where the offender has fraudulently obtained or wrongfully disclosed records, § 4-309 (e) or knowingly violated any provision of the act, § 4-309 (f).

105. While GRMC is not alleged to have met these additional criteria, they are in general violation of the act as described in § 4-309 (c) (2) because they failed in their duty to keep the medical record confidential as required in § 4-302 (a).

106. § 4-301 (k) (4) (i) contains specific provisions concerning minors.

107. The violation of Maryland Medical Records Act by GRMC caused Plaintiff to suffer harm as described above and actual damages in an amount to be determined at trial.

COUNT III – ACTION FOR VIOLATION OF MARYLAND PERSONAL INFORMATION PRIVACY ACT (“PIPA”), MD. COMM. CODE §§ 14-3504

108. Plaintiff realleges and incorporates by reference each and every allegation set forth

above.

109. While compliance with HIPAA would satisfy obligations under MD PIPA, failure to comply with HIPAA should not provide relief from obligations under this State code.

110. Additionally, because some of Plaintiff's information that was illegally accessed and disclosed was outside the scope of HIPAA but properly within the scope of MD PIPA.

111. Per Maryland §14-3501 (d) "Health information" means any information regarding an individual's medical history, medical condition, or medical treatment or diagnosis.

112. Per Maryland §14-3501 (e) (1), "Personal information" (PI) means: (i) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable:

1. A Social Security number, an Individual Taxpayer Identification Number, a passport number, or other identification number issued by the federal government;
2. A driver's license number or State identification card number;
3. An account number, a credit card number, or a debit card number, in combination with any required security code, access code, or password, that permits access to an individual's financial account;
4. Health information, including information about an individual's mental health;
5. A health insurance policy or certificate number or health insurance subscriber identification number, in combination with a unique identifier used by an insurer or an employer that is self-insured, that permits access to an individual's health information.

113. Per Maryland §14-3501 (e) (2) (iii) "Personal information" does not include: Information that is disseminated or listed in accordance with the federal Health Insurance Portability and Accountability Act.

114. Per Maryland §14-3507 (d) (1) “A business that is subject to and in compliance with the federal Health Insurance Portability and Accountability Act of 1996 shall be deemed to be in compliance with this subtitle.”

115. Under HIPAA, Protected health information (PHI) means individually identifiable health information.

116. Under HIPAA, Health Information means any information, including genetic information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

117. According to the National Institute of Standards and Technology (NIST), Personally Identifiable Information (PII) is — “any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information”

118. PII includes, but is not limited to, Social Security numbers, passport numbers, driver’s license numbers, addresses, email addresses, photos, biometric data, or any other information that can be traced to one individual. Medical, educational, financial, and employment information all fall under PII.

119. Protected health information is a *subset* of PII. PHI specifically refers to health information shared with HIPAA covered entities, including medical records, lab reports, and

hospital bills, along with any information relating to an individual's past, present, or future physical or mental health.

120. Therefore, some PII is not PHI and in this case some of PII affected by Defendant's actions were outside the scope of the provisions of HIPAA.

121. The actions of Defendant described in this complaint constitute breach of a security system under §14–3504.

122. GRMC violated PIPA because it did not provide notice of the breach of its security in accordance with the requirements of §14–3504.

123. None of the communications from GRMC to Plaintiff following the breach included all of the information required in §14–3504.

124. GRMC also failed to provide notice to the Maryland Attorney General of the incident, as required by §14–3504.

125. A violation of PIPA is an unfair or deceptive trade practice.

126. Through GRMC's actions alleged above, Plaintiff suffered actual damages in an amount to be determined at trial.

COUNT IV – ACTION FOR NEGLIGENCE *PER SE*

127. Plaintiff realleges and incorporates by reference each and every allegation set forth above.

128. Under HIPAA, GRMC is required to "ensure the confidentiality, integrity, and availability of all electronic protected health information" and this responsibility includes ensuring compliance by its workforce. See 42 U.S.C. § 1320d-6. Both aspects were violated.

129. Because GRMC failed to comply with HIPAA, that statute does not provide a safe haven for determining compliance and enforcement of related Maryland statutes. Therefore,

Defendant violated Maryland Personal Information Privacy Act §14-3504.

130. Defendant is liable for negligence against Plaintiff due to violation of each of the above statutes as negligence per se.

131. The content of these statutes constitute legal duties owed by Defendant to Plaintiff, and the violation of these laws is evidence these duties were breached.

132. The Plaintiff is within the class of persons intended to be protected by these statutes.

133. The damages suffered by Plaintiff due to the violation of these statutes were exactly the type of harms the statutes were intended to prevent.

134. The violations of these statutes were the proximate cause of Plaintiff's injuries as detailed herein.

135. Through Defendant's actions alleged above, Plaintiff suffered actual damages in an amount to be determined at trial.

COUNT V – ACTION FOR BREACH OF IMPLIED CONTRACT

136. Plaintiff realleges and incorporates by reference each and every allegation set forth above.

137. GRMC's "Patient Rights and Notice of Privacy Practice" includes the following statement:

"In adherence with state and federal requirements, Garrett Regional Medical Center is committed to protecting patient privacy. Protected health information will not be disclosed for any other purposes unless a patient gives permission to release the information, or reporting is required by law. Patient medical information contained in medical records is confidential and will be used only for the purposes of treatment, payment, or healthcare operations."

See <https://wvumedicine.org/garrett-regional-medical-center/patients-visitors/notice-of-privacy-practice/>.

138. Through its course of conduct, GRMC and Plaintiff entered into an implied contract for GRMC to implement data security adequate to safeguard and protect the privacy of Plaintiff's PHI/PII and financial information.

139. GRMC required Plaintiff to provide and entrust his PHI/PII and financial information as a condition of obtaining GRMC's services.

140. GRMC solicited and invited Plaintiff to provide his PHI/PII and financial information as part of GRMC's regular business practices.

141. Plaintiff accepted GRMC's offers and provided his PHI/PII and financial information to GRMC.

142. As a condition of being a patient of GRMC, Plaintiff provided and entrusted his PHI/PII and financial information to GRMC.

143. In so doing, Plaintiff entered into an implied contract with GRMC by which GRMC agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff if his data had been breached and compromised or stolen.

144. A meeting of the minds occurred when Plaintiff agreed to and did provide his PHI/PII and financial information to GRMC in exchange for, amongst other things, the protection of his PHI/PII and financial information.

145. Plaintiff fully performed his obligations under the implied contract with GRMC.

146. GRMC breached its implied contract with Plaintiff by failing to safeguard and protect his PHI/PII and financial information and by failing to provide timely and accurate notice to him that his PHI/PII and financial information was compromised.

147. As a direct and proximate result of GRMC's above-described breach of implied

contract, Plaintiff suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

148. Through Defendant's actions alleged above, Plaintiff suffered actual damages in an amount to be determined at trial.

COUNT VI – ACTION FOR VIOLATION OF MARYLAND CONSUMER PROTECTION ACT (“CPA”), MD. COMM. CODE §§ 13-301.

149. Plaintiff realleges and incorporate by reference each and every allegation set forth above.

150. GRMC has engaged in unfair or deceptive trade practices, in violation of Maryland Code, Commercial Law Article §§ 13-301 and 13-303.

151. GRMC engaged in and carried out unfair and deceptive trade practices. Among other things, GRMC made false and misleading statements in connection with the security and privacy protections provided in use of its electronic medical records system.

152. As described above, violation of the MD PIPA constitutes a violation of the CPA under §14-3508.

153. Through Defendant's actions alleged above, Plaintiff suffered actual damages in an amount to be determined at trial.

154. Plaintiff should also be awarded attorneys' fees as authorized by Maryland Code, Commercial Law § 13-408(b).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Brandon Lee Roane, on behalf of himself and all others similarly situated, respectfully requests the following relief:

- A. For an Order certifying the instant matter as a class action;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct described above;
- C. For compensatory damages;
- D. For reasonable attorney's fees and costs; and
- E. For such other and further relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, Brandon Lee Roane, pursuant to Md. Rule 2-325, demands a trial by jury of all issues so triable.

/s/ Arnold J. Abraham
Arnold J. Abraham, Esq.
MD Bar No 1706200002
CyberLaw, LLC
220 N. Liberty Street
Baltimore MD 21201
Phone: (443) 906-3495

Eric Menhart, Esq.
MD Bar No 060613015
Lexero Law
512 C Street, NE
Washington, DC 20002
Phone: (855) 453-9376

ATTORNEYS FOR PLAINTIFF